Allgemeine Bestimmungen der DeepCloud AG für die Nutzung von DeepID (Januar 2024)

1. Allgemeines

1.1 Dies sind die Allgemeinen Bestimmungen (**AB**) der DeepCloud AG, Abacus-Platz 1, 9300 Wittenbach, Schweiz (**DeepCloud**) für die Nutzung des Dienstes DeepID und der dazugehörigen DeepID App (**DeepID**).

1.2 DeepID ermöglicht die Feststellung der Identität einer natürlichen Person (**Identifikation**), die Einladung weiterer Personen zu ihrer Identifikation (damit sie - als Unterschriftsberechtigte - eine Organisation verifizieren können), die **Autorisierung** gewisser Willensbekundungen (wie die Freigabe bestimmter elektronischer Signaturen) oder Handlungen sowie die **Authentisierung und Authentifizierung** bei bestimmten Anwendungen von DeepCloud oder Drittanbietern. Für Leistungen, die von einem Drittanbieter unter Einsatz von DeepID genutzt werden, kommt ein Vertrag ausschliesslich zwischen dem Nutzer von DeepID (**Nutzer**) und dem jeweiligen Drittanbieter zustande.

1.3 Mit diesen AB regelt DeepCloud Rechte und Pflichten sowie weitere massgebliche Aspekte im Zusammenhang mit der Nutzung von DeepID.

1.4 Die Zustimmung des Nutzers zu diesen AB erfolgt im Rahmen des Identifikationsprozesses in der DeepID App. Damit erklärt er, berechtigter Besitzer des Authentisierungsmittel (wie ein Smartphone, Tablet) zu sein und die alleinige Kontrolle über dieses Authentisierungsmittels zu haben, sowie dass ihm die Rechte und Pflichten gemäss AB bekannt sind, er mit diesen einverstanden ist und er die AB einhalten wird. Er sichert zu, dass er volljährig ist und über die nötige Geschäftsfähigkeit verfügt, um sich zur Einhaltung dieser AB zu verpflichten. Minderjährige zwischen 16 und 18 Jahren sorgen für die erforderliche Einwilligung der Erziehungsberechtigten.

2. Leistungen von DeepCloud

2.1 DeepCloud stellt dem Nutzer mit DeepID einen Identifikations-, Verifikations-, Autorisierungs- und Authentisierungsdienst für unterschiedliche Anwendungsfälle zur Verfügung.

2.2 Hierfür bietet DeepCloud die DeepID App an. Sie kann aus den entsprechenden App-Stores heruntergeladen werden.

3. Identifikation des Nutzers mittels der DeepID App

3.1 Vor der erstmaligen Nutzung der Funktionalitäten der DeepID muss die Identität des Nutzers bestätigt werden. Dafür folgt der Nutzer den in der DeepID App vorgesehenen Schritten. Er gibt seine Nationalität und seinen Wohnsitz an und präsentiert ein gültiges Ausweispapier. Er bestätigt den Besitz und die alleinige Kontrolle über sein Gerät durch Eingabe des ihm per E-Mail zugesendeten vierstelligen Codes in der DeepID App. Während des Prozesses definiert er seinen Geräte-PIN, wobei er für das DeepID Login optional auch den Zugriffschutz seines Gerätes (wie Geräte-Biometrie (Fingerabdruck / Gesichtserkennung) oder PIN-Code) verwenden kann.

3.2 Nach vollständiger Bestätigung der Identität des Nutzers mit Hilfe eines gültigen Ausweispapiers und allfälliger Kontrollen kann er seine DeepID per App nutzen. Sie wird als solche mit allen Rollen und Attributen (mit ID- und Zugangsdaten) gespeichert.

3.3 Beim Erfassen und Verarbeiten der Daten des Nutzers im Rahmen des Identifikationsprozesses werden von ihm ebenfalls biometrische Daten aus den erstellten Fotos und Videos sowie aus seinem Ausweispapier gewonnen und verglichen. Nur so kann der Nachweis der Identität verlässlich durchgeführt werden. Der Nutzer stimmt hiermit ausdrücklich der Verarbeitung seiner biometrischen Daten für die Feststellung seiner Identität zu.

3.4 Der detaillierte Ablauf des Identifikationsprozesses und welche Daten dabei erhoben und verarbeitet werden, sind in der Datenschutzerklärung von DeepCloud im Abschnitt «Datenverarbeitungen bei Nutzung unserer mobilen Applikationen (Apps)» unter «DeepID Dienst und Mobile App DeepID (Android und iOS)» beschrieben. DeepCloud hat das Recht, die Abläufe bei der Identitätsfeststellung aus berechtigten Gründen anzupassen und zu ändern. Der Nutzer sollte aus diesem Grund die Datenschutzerklärung von DeepCloud in regelmässigen Abständen zur Kenntnis nehmen, um allfällige Änderungen zu erfahren.

3.5 Möchte der Nutzer seine bestätigte DeepID Identität für Dienste von Drittanbietern nutzen, kann es je nach Dienst aufgrund unterschiedlicher Nutzungsbedingungen gewisse Einschränkungen oder Bedingungen geben. Diese sind einzuhalten.

3.6 Der Nutzer hat im Rahmen des Identifikationsprozesses bestimmte Daten anzugeben und Fotos und Videos von sich und seinem Ausweispapier zu erstellen. Fotos und Video sind zwingend eigenhändig vom Nutzer und durch ihn selbst aufzunehmen.

3.7 Der Nutzer hat alle durch ihn erfassten und angezeigten Daten auf Lese- bzw. Schreibfehler zu überprüfen oder nicht erfolgreich beendete Schritte (wie Foto- und Videoerstellung) nach Aufforderung zu wiederholen, andernfalls kann der Prozess nicht abgeschlossen werden. Er ist verantwortlich für die Präsentation vollständiger, korrekter und aktueller Daten hinsichtlich seiner Person. Besonders die Details zu seiner Identität, wie aus dem Ausweispapier sowie nach seinen Angaben, sind zu bestätigen und erforderlichenfalls zu korrigieren.

3.8 Es ist erforderlich, dass das Gerät des Nutzers nach den vorgegebenen Anforderungen als sein Authentisierungsmittel für die Nutzung von DeepID registriert wird. Der Nutzer bestätigt damit, dass er berechtigter Besitzer des Authentisierungsmittel (wie ein Smartphone, Tablet) ist und die alleinige Kontrolle über dieses hat.

3.9 Zur Steigerung der Sicherheit der DeepID App hat der Nutzer die angeforderten Sicherheitsvorgaben (wie Aktivierung des Zugriffsschutzes) einzuhalten. Er legt hierfür eine 6-stellige PIN fest, aktiviert den Zugriffsschutz des Gerätes (wie Face-ID, Fingerabdruck) sowie die automatische Bildschirmsperre zum Entsperren der DeepID App. Ausserdem erhält er seitens DeepCloud einen Wiederherstellungscode, der sicher zu verwahren ist. Nur mit diesem kann in bestimmten Fällen Zugriff auf DeepID wiederhergestellt werden. Es besteht die Möglichkeit, einen neuen Wiederherstellungscode zu generieren.

3.10 Die Identifikation des Nutzers erfordert die Erfüllung bestimmter Anforderungen, die geprüft und bestätigt werden müssen (wie Ausweispapier, Foto, Video). Die Überprüfung erfolgt entweder vollautomatisch bei Vorliegen der entsprechenden Voraussetzungen, andernfalls nur zu den üblichen Bürozeiten von DeepCloud. Der Nutzer hat dies entsprechend einzuplanen, möchte er mittels DeepID beispielsweise elektronische Signaturen fristgerecht erteilen. DeepCloud setzt hierfür Personen ein, die speziell für den Identifikationsprozess ausgebildet werden. Unter Umständen sind weitere Abklärungen erforderlich. Hierüber wird der Nutzer durch den Support (wie innerhalb der DeepID App, per E-Mail) informiert.

3.11 Nach Bestätigung seiner Identität kann der Nutzer die Funktionalitäten von DeepID nutzen, in den Einstellungen zwischen verschiedenen Settings wählen (wie Anpassung der Profildaten, Gerätesicherungseinstellung, PIN-Änderung, Aktualisierung des Ausweispapiers) oder sich aus DeepID ausloggen.

3.12 Nach dem Ausloggen oder bei 3fach-falscher PIN-Eingabe hat der Nutzer die von der DeepID App vorgesehenen Schritte zu befolgen, um sich wieder in der DeepID App einloggen zu können.

3.13 In gewissen Fällen ist eine erneute Identifikation (**Re-Identifikation**) des Nutzers erforderlich, wie bei Änderungen hinsichtlich des verwendeten Ausweispapiers (wie Foto, Name, Geschlecht, Nationalität, Ablauf der Gültigkeitsdauer des Ausweispapiers, Verlust des Ausweispapiers, Änderungen im NFC-Code), Ablauf der Gültigkeitsdauer der festgestellten Identität für elektronische Signaturen, Änderung des Gerätes, das als Authentisierungsmittel für DeepID dient (wie bei Diebstahl, Verlust, Wechsel), sowie bei Ablauf der Gültigkeitsdauer der DeepID Identität und bei jedem Umstand, der für die Feststellung der Identität des Nutzers relevant ist. Hierfür wählt der Nutzer die Funktion «Ich habe bereits eine DeepID» oder «Dokument erneuern» und befolgt den vorgegebenen Identifikationsprozess.

3.14 DeepCloud ist jederzeit berechtigt, einen Identifikationsprozess mit dem Nutzer auszusetzen oder (auf Dauer) zu beenden (z.B. bei Widersprüchen in den Angaben, Undurchführbarkeit der Identifikation) oder aus berechtigten Gründen eine bestätigte DeepID Identität für ungültig zu erklären. Daraus ergeben sich für den Nutzer keinerlei Ansprüche (wie auf Schadensersatz) oder andere Rechte.

4. Funktionalitäten der DeepID App

4.1 In der DeepID App sind alle Funktionalitäten für den Nutzer ersichtlich, dazu gehören «Scan QR Code», «Verlauf», «Organisationen», «Dokument erneuern» oder «Signaturen». DeepCloud ist jederzeit berechtigt, bestehende Funktionalitäten zu ändern oder zu beenden sowie neue Funktionalitäten hinzuzufügen.

4.2 Der Nutzungsumfang von DeepID setzt sich aus der Nutzungsüberlassung der hierfür erforderlichen Software im Rahmen der hierin eingeräumten Nutzungsrechte einschliesslich der Speicherung der Daten zusammen. Die nach DeepID bestätigte Identität kann sowohl direkt über die DeepID App sowie für andere Anwendungen von DeepCloud als auch über die Integration von Anwendungen, Software oder Applikationen, auch von Drittanbietern, genutzt werden.

4.3 Die **Funktionalität «Scan QR-Code»** ermöglicht dem Nutzer das Scannen eines QR-Codes und die Vornahme der darin enthaltenen Aktion. Hierzu können die Autorisierung (wie die Freigabe einer Willensbekundung oder Handlung) oder die Authentisierung für einen DeepCloud- oder Drittanbieterdienst (wie ein Login, eine Identitätsbestätigung oder ein Systemzugriff) gehören.

4.4 Die **Funktionalität «Signatur Verlauf»** listet die mittels DeepID erfolgten Aktionen, wie die Abgabe einer elektronischen Signatur.

4.5 Die **Funktionalität «Organisationen»** ermöglicht dem identifizierten Nutzer weitere Personen einzuladen, um ebenfalls den Identifikationsprozess per DeepID zu durchlaufen. Zweck der Einladungen ist es, dass für eine Organisation unterschriftsberechtigte Personen identifiziert werden, wodurch die Organisation verifiziert werden kann. Hierfür hat der Nutzer ein DeepCloud-Konto bei DeepCloud zu eröffnen. Darin kann er Personen einladen, die anschliessend eigenständig den Identifikationsprozess von DeepID durchlaufen, wobei erteilte Angaben mit öffentlichen Quellen abgeglichen werden.

4.6 Mit der **Funktionalität «Dokument erneuern»** ist der Nutzer verpflichtet, eine Re-Identifikation bei relevanten Änderungen selbstständig und zeitnah vorzunehmen. Er wird hierdurch an die Re-Identifikation erinnert, wenn sein für die Identifikation genutztes Ausweispapier oder ein Zertifikat für seine elektronische Signatur seine Gültigkeitsdauer verliert. Dafür hat er den Identifikationsprozess erneut zu durchlaufen. Der Nutzer ist mit dieser Erinnerung in der DeepID App sowie per E-Mail einverstanden.

4.7 Die **Funktionalität «Task»** ermöglicht dem Nutzer die Freigabe von fortgeschrittenen und qualifizierten elektronischen Signaturen, die ihm von einer Zertifizierungs- bzw. Vertrauensdiensteanbieterin zur Verfügung gestellt werden.

5. Einsatzmöglichkeiten der DeepID Identität

5.1 Die mittels DeepID bestätigte Identität kann für unterschiedliche Anwendungszwecke, zusammen mit dem Authentisierungsmittel, für Autorisierungen und Authentifizierungen genutzt werden.

5.2 Eine Anfrage zur Nutzung erfolgt durch einen DeepService oder von einem Drittanbieter ausserhalb der DeepID App (wie die Einladung zur Abgabe einer elektronischen Signatur), wobei die jeweiligen Bestimmungen des Drittanbieters oder von DeepCloud für diesen Dienst zu akzeptieren und einzuhalten sind.

5.3 Falls bei einer Anfrage noch keine gültige Identifikation vorliegt, wird der Nutzer aufgefordert, sich zu identifizieren. Sollte bereits eine gültige Identifikation vorliegen, jedoch das benutzte Gerät neu sein oder die Ausweispapiere erneuert werden müssen (nach maximal 5 Jahren oder nach Ablauf ihrer Gültigkeit, was immer zuerst eintritt) ist eine Re-Identifikation oder die Erneuerung der Dokumente erforderlich.

5.4 Die konkret geforderte Aktion hängt vom jeweiligen Dienst und der gewählten Einsatzmöglichkeit ab. DeepID dient lediglich der Ermöglichung des anderen Dienstes. Für die Leistungen, die der Nutzer bei einem Drittanbieter unter Einsatz der DeepID Identität nutzt (z.B. als Identifizierungsmittel bei Anmeldung zu einem gesicherten Zugang oder für die Abgabe einer elektronischen Signatur), kommt für diesen Dienst ein Vertrag zwischen dem Nutzer und dem jeweiligen Drittanbieter zustande. Aus den Vertragsbestimmungen dieser Drittanbieter können sich Einschränkungen zur Nutzung von DeepID für ihre Dienste ergeben.

5.5 Voraussetzung für die Nutzung des Drittanbieterdienstes ist, dass sich der Nutzer erfolgreich mittels DeepID App identifiziert hat, die DeepID Identität von diesem Drittanbieter akzeptiert wird und bei DeepID angeschlossen ist sowie, dass der Nutzer die Freigabe der jeweiligen Anfrage erteilt.

5.6 Die DeepID App überträgt die im Identifikationsprozess erhobenen Inhalte an DeepCloud respektive an die für die Identifikation eingebundenen Auftragsverarbeiter sowie - bei einer Anfrage - die hierfür erforderlichen Inhalte an einen berechtigten Drittanbieter zur Authentifizierung des Nutzers und der Ausführung der jeweils angefragten Aktion. Dabei kann ein Informationsaustausch mit oder zwischen Systemen eines Drittanbieters stattfinden oder Inhalte mit diesen synchronisiert werden. Hierfür sind den beteiligten Parteien die erforderlichen Zugriffe, der Austausch zwischen den jeweiligen Systemen sowie die Verarbeitung der Inhalte ausdrücklich gestattet. Dabei können personenbezogene Daten, Dokumente sowie Transaktionsdaten übermittelt und verarbeitet werden. Der Nutzer stimmt dem hiermit ausdrücklich zu.

5.7 Der Ablauf eines Autorisierungs- bzw. Authentifizierungsprozesses für einen Dienst ist der Folgende: Der Nutzer erhält vom jeweiligen Dienst eine Anfrage (per E-Mail, Push-Benachrichtigung, SMS, etc.), um die Freigabe innerhalb der DeepID App auf seinem Authentisierungsmittel zu geben. Hierfür steht ein gewisser Zeitrahmen zur Verfügung, der je nach Dienst unterschiedlich lang sein kann. Nach Anmeldung in der DeepID App kann der Nutzer die angeforderte Freigabe wie eine elektronische Signatur oder andere Aktion (z.B. Anmeldung zu Anwendungen oder Logins, Weitergabe von Daten) erteilen. Sobald der Nutzer die Freigabe erteilt, wird diese Information mit einem kryptographischen Schlüssel, der auf dem Authentisierungsmittel gespeichert ist, digital signiert und der jeweilige Diensteanbieter erhält mit verschlüsselter Übertragung die Bestätigung, dass die Freigabe vom berechtigten Gerät aus versendet wurde (der Dienstanbieter kann mit dem öffentlichen kryptographischen Schlüssel die signierte Information prüfen). Somit kann davon ausgegangen werden, dass die Freigabe von der richtigen Person gegeben wurde, und die angefragte Handlung kann gewährt werden.

5.8 Hat der Nutzer die Freigabe nicht oder nicht rechtzeitig erteilt, erhält der Diensteanbieter die Information, dass die Freigabe nicht erteilt wurde und die Autorisierung fehlt oder die Authentifizierung nicht erfolgreich war. DeepID ermöglicht hierbei lediglich die Autorisierung oder Authentifizierung des Nutzers für Dienste von Drittanbietern, die die DeepID Identität akzeptieren. Sollte der Nutzer nicht oder nicht rechtzeitig die angeforderte Aktion autorisieren, ist er selbst für die daraus resultierenden Folgen verantwortlich.

5.9 Die DeepID App unterstützt die Multi-Faktor-Authentifizierung. Dadurch wird das gewünschte Gerät mittels des Identifikationsverfahrens als zusätzlicher Faktor legitimiert und kann für die Bestätigung der angefragten Aktion eingesetzt werden. Die Zwei-Faktor-Authentifizierung ist eine Sicherheitsprozedur, bei der der Nutzer zwei unterschiedliche Merkmale bereitstellt, um sich auszuweisen oder eine explizite Willensbekundung abzugeben. Im Fall von DeepID ist es der Besitz des Authentisierungsmittels sowie bei Autorisierung oder Authentisierung als zweite Komponente die DeepID App zur Bestätigung der Aktion.

5.10 Im Rahmen des Identifikationsprozesses wird das benutzte Gerät durch den Einsatz der KI-basierten, nutzerzentrierten Authentifizierungssuite authentisiert und kann so für Autorisierungen und Authentisierungen für eine Kommunikation zum Drittanbieter genutzt werden.

6. Einsatzmöglichkeiten der DeepID Identität bei elektronischen Signaturen

6.1 Die DeepID Identität kann zur Autorisierung und Authentifizierung von fortgeschrittenen und qualifizierten elektronischen Signaturen verwendet werden. Anerkannte Zertifizierungs- bzw. Vertrauensdiensteanbieterinnen (Anbieterinnen) können einer identifizierten Person fortgeschrittene Zertifikate für fortgeschrittene elektronische Signaturen (FES) und qualifizierte Zertifikate für qualifizierte elektronische Signaturen (QES) mit qualifiziertem Zeitstempel (Zertifizierungs- bzw. Vertrauensdienste) ausstellen. Es gilt, dass sich ein Nutzer einmal identifizieren muss, um mehrfach signieren zu können, mit Ausnahme einer erforderlichen Re-Identifikation.

6.2 Die DeepID App ermöglicht die hierfür notwendige Prüfung der Identität dieser Person (**Signierender**). Diese Zertifizierungs- bzw. Vertrauensdienste werden gemäss schweizerischem Bundesgesetz über die elektronische Signatur (**ZertES**) bzw. gemäss der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (**eIDAS VO**) von diesen Anbieterinnen erbracht.

6.3 DeepCloud ist von diesen Anbieterinnen beauftragte Registrierungsstelle für QES und FES. Sie unterliegt dem jeweils aktuell gültigen DeepCloud Trust Service Practice Statement (TSPS). Ihre Konformität mit dem TSPS wurde durch eine anerkannte Zertifizierungsstelle (Conformity Assessment Body/CAB) in der Schweiz und der EU bewertet und bestätigt. DeepCloud wurde nach folgendem Konformitätsbewertungsschema zertifiziert (Norm of Accreditation System): ISO 17021-1:2015 (für ZertES) und ISO 17065-1:2013 (für eIDAS VO) für «Remote Identification Certification» nach den Anforderungen von ZertES, VZertES, TAV (SR 943.032.1), EU eIDAS VO, ETSI TS 119 461, ETSI EN 319 401 und ETSI EN 419 241-1.

6.4 DeepCloud prüft im Rahmen eines zertifizierten Identifikationsprozesses mit DeepID die Identität des Signierenden, ohne dass dieser anwesend sein muss. Hierbei sind die Vorgaben durch den Nutzer genau zu befolgen und stets vollständige, richtige und aktuelle Angaben zu machen. Im Identifikationsprozess kann der Nutzer aufgefordert werden, unterschiedliche Dokumente vorzulegen, je nach dem, wofür die Identifikation verwendet wird.

6.5 Sollte eine Identifikation nicht erfolgreich durchgeführt werden können, hat DeepCloud das Recht, einen erneuten Identifikationsversuch kurzzeitig oder auf Dauer auszuschliessen. Falls die Identifikation alle erforderlichen Voraussetzungen erfüllt, wird die DeepID Identität für die Erstellung von FES und QES registriert. Diese Registrierung wird vor jeder Beauftragung des Signierenden neu geprüft.

6.6 Insbesondere bestehen bei Beauftragung der Ausstellung von FES oder QES vor ihrer Freigabe durch den Signierenden Besonderheiten. So muss der Signierende seinen Wohnsitz in der Schweiz, der EU oder des EWR haben und dies bei Beauftragung der Erstellung der QES und FES bestätigen. Ist dies nicht der Fall, darf der Nutzer diese Dienste nicht in Anspruch nehmen. Er haftet vollumfänglich für mögliche Folgen aus der Nichteinhaltung dieser Anforderungen. DeepCloud und die jeweiligen Drittanbieter schliessen in solchen Fällen jede Gewähr und Haftung hinsichtlich ihrer Dienste aus.

6.7 Für die Identifikation zur Beauftragung einer QES und FES sind ausschliesslich solche Ausweispapiere zugelassen, die die Anbieterinnen der Zertifizierungs- bzw. Vertrauensdienste hierfür erlauben. Diese ergeben sich aus dem Identifikationsprozess. Die Ausweispapiere müssen zum Zeitpunkt der Identifikation gültig sein. Die Liste der zugelassenen Ausweispapiere kann sich ändern, so dass ggf. eine Re-Identifikation erforderlich wird. Es dürfen zur Identifikation und bei Beauftragung durch den Signierenden nur die von den Anbieterinnen der Zertifizierungs- bzw. Vertrauensdienste vorgegebenen Ausweispapiere verwendet werden. Sie legen ebenfalls fest, ob der Signierende einen Identifikationsprozess für jede elektronische Signatur durchlaufen muss (Einmalsignatur) oder ob er nach dem Identifikationsprozess während einer bestimmten Dauer mehrere elektronische Signaturen erstellen kann. Hieraus kann sich gegebenenfalls die Erforderlichkeit einer Re-Identifikation des Signierenden ergeben.

6.8 Der Signierende wird zur Erteilung einer elektronischen Signatur mittels eines Dienstes (wie DeepSign, dem Signatur-Dienst von DeepCloud) eingeladen. Je nach Auswahl der gewünschten Signaturart soll entweder eine einfache elektronische Signatur (EES) oder eine QES bzw. FES nach den jeweils anwendbaren gesetzlichen Bestimmungen (ZertES oder eIDAS VO) erteilt werden. Eine andere Nutzungsart als die Beauftragung der angebotenen Zertifizierungs- bzw. Vertrauensdienste dieser Anbieterinnen ist nicht zulässig (Nutzungsbeschränkung).

6.9 DeepCloud registriert und speichert die im Identifikationsprozess DeepID zur Person des Nutzers erhobenen Angaben und die im Freigabeprozess für die Zertifizierungs- bzw. Vertrauensdienste erforderlichen Inhalte gemäss vertraglichen Regelungen und geltenden Vorschriften.

6.10 Die Anbieterinnen sind für die Erstellung der Zertifikate und für das kryptographische Schlüsselpaar für den Signaturvorgang nach Erteilung der Freigabe durch den Nutzer verantwortlich. Der Signierende darf zusammen mit seinen Aktivierungsdaten unter Einsatz von DeepID dieses Zertifikat verwenden. Sobald der Signierende nach entsprechender Beauftragung (unter Akzeptanz der Nutzungsbestimmungen der jeweiligen Anbieterin und der Bestätigung des geforderten Wohnsitzes) seine Freigabe in DeepID erteilt hat, erstellt die jeweilige Anbieterin für ihn die FES oder QES basierend auf diesem Zertifikat. Für jeden Signaturvorgang wird ein neues digitales Zertifikat (mit einer kurzen Gültigkeitsdauer) mit einem neuen Schlüsselpaar erstellt.

6.11 Mit der bestätigten Identifikation mittels DeepID kann der Nutzer den jeweiligen Zertifizierungs- bzw. Vertrauensdienst für die Gültigkeitsdauer der Identifikation bei allen Signaturapplikationen, die DeepCloud und die Anbieterinnen mit DeepID verbunden haben, nutzen, um eine gültige QES oder FES erstellen zu lassen, ohne dass eine erneute Identifikation notwendig ist, solange dies von der jeweiligen Signaturapplikation und der Gültigkeitsdauer des Zertifikats zugelassen wird.

6.12 DeepCloud wird die Identität des Signierenden überprüfen, ihn authentisieren und ihm die Autorisierung ermöglichen.

6.13 Die Anbieterinnen sind berechtigt, bei DeepCloud die Einhaltung ihrer vertraglichen Pflichten bei der Identifikation, Autorisierung und Authentifizierung für FES und QES durch Auditierung zu überprüfen. Dabei können ebenfalls Daten des Signierenden eingesehen werden. Sie können dies durch eigene Mitarbeitende oder durch Dritte ausführen lassen und die Ergebnisse mit zuständigen Konformitätsbewertungsstellen und Aufsichtsbehörden teilen.

7. Nutzungsrechte, Immaterialgüterrechte

7.1 DeepCloud gewährt dem Nutzer ein persönliches, nicht exklusives, nicht übertragbares, nicht abtretbares, einfaches, räumlich und zeitlich beschränktes Nutzungsrecht an der eingesetzten Software bei Nutzung von DeepID für die Dauer des Nutzungsverhältnisses zur Eigennutzung auf seinem Authentisierungsmittel. Dies bedeutet, dass nur der Nutzer selbst für sich DeepID nutzen darf. Der Umfang des Nutzungsrechts ergibt sich aus diesen AB.

7.2 Dem Nutzer ist es untersagt, DeepID Dritten zugänglich zu machen oder zur Verfügung zu stellen. Darüber hinaus ist er nicht berechtigt, die eingesetzte Software für eine andere Nutzung als die von DeepCloud hierin gewährte einzusetzen.

7.3 DeepCloud hat das Recht, Schnittstellen anzubieten und zu lizenzieren, um Daten aus DeepID in andere Systeme zu exportieren, die dort weiterverarbeitet werden könnten. Der Nutzer darf solche Schnittstellen zu Diensten, auch von Drittanbietern, nur im Rahmen dieses Nutzungsverhältnisses in Anspruch nehmen. Dies betrifft auch den Fall, wenn Schnittstellen mit dem Zweck verwendet werden, Daten mittels eines anderen Systems zu nutzen. Der Nutzer hat die durch DeepCloud vorgegebenen Nutzungsmöglichkeiten und Limite einzuhalten und ist nicht berechtigt, diese durch technische Ausweichmöglichkeiten zu umgehen.

7.4 Die bei DeepCloud verwendete Software kann Exportkontrollvorschriften und anderen Gesetzen unterliegen. Sie darf in einem solchen Fall nicht in gewisse Länder oder an Personen oder Rechtssubjekte, denen der Erhalt von gewissen Exportwaren untersagt ist (einschliesslich derer, die auf den einschlägigen Sanktionslisten für Personen bzw. Rechtsubjekte aufgeführt sind), ex-portiert, re-exportiert oder transferiert werden. Der Nutzer hat allfällige lokale Vorschriften im Zusammenhang mit der Nutzung von Diensten mit Verschlüsselungstechnik, wie sie für DeepID verwendet wird, zu beachten.

7.5 In Bezug auf eingesetzte Software von Drittanbietern gelten deren Lizenzbestimmungen.

7.6 Der Nutzer unterrichtet DeepCloud unverzüglich, falls Dritte Schutzrechte (z.B. Urheber- oder Patentrechte) gegen ihn geltend machen, die sich auf Software bei Nutzung von DeepID beziehen. Er unternimmt ohne Ermächtigung von DeepCloud keine rechtlichen Schritte und darf von sich aus keine Ansprüche von Dritten ohne Zustimmung von DeepCloud anerkennen. DeepCloud unternimmt alle erforderlichen Verteidigungsmassnahmen, wie die Abwehr von Ansprüchen Dritter, auf eigene Kosten, soweit sie nicht auf pflichtwidrigem Verhalten des Nutzers beruhen.

7.7 Der Nutzer nimmt zur Kenntnis, dass sein App-Store in keiner Weise verpflichtet ist, Wartung und Support-Leistungen betreffend der DeepID App zu leisten. Macht ein Dritter geltend, DeepID oder der Besitz der DeepID App verletze seine Immaterialgüterrechte, ist DeepCloud und nicht der App-Store für die Abwehr dieser Ansprüche zuständig.

7.8 Alle Immaterialgüterrechte an DeepID (inkl. der hierfür verwendeten Software), an Inhalten, Texten, Bildern, Fotos, Videos, Logos oder anderen Informationen von DeepCloud, einschliesslich ihrer Webseiten, gehören ausschliesslich DeepCloud oder den jeweiligen Rechteinhabern. Für jede weitergehende Nutzung jeglicher Immaterialgüterrechte ist die schriftliche Einwilligung der Rechteinhaber im Voraus einzuholen. Alle Dokumentationen von DeepCloud, die im Rahmen des Nutzungsverhältnisses zugänglich gemacht werden, gelten als ihr geistiges Eigentum.

7.9 DeepCloud ist berechtigt, Fotos und Videos ohne Vergütungsanspruch des Nutzers für den Identifikationsprozess oder als gewähltes Profilbild zu verarbeiten.

8. Nutzungsvoraussetzungen und Pflichten des Nutzers

8.1 Der Nutzer verfügt über ein Gerät, das als zugelassenes Authentisierungsmittel dient, und bestätigt seine Identität mit der DeepID App. Die Nutzung der DeepID App setzt voraus, dass das verwendete Gerät die erforderlichen Geräte- und Systemvoraussetzungen dauerhaft erfüllt.

8.2 Er ist verantwortlich für sein verwendetes Authentisierungsmittel, das nur ihm zur Nutzung zur Verfügung steht. Solange er DeepID nutzen möchte, ist es ihm untersagt, das Authentisierungsmittel Dritten zu überlassen.

8.3 Die Software des Authentisierungsmittels muss auf dem neuesten Stand gehalten werden. Insbesondere müssen die vom Hersteller zur Verfügung gestellten Aktualisierungen (Updates, Upgrades, Service Packs, Hotfixes etc.) sowie die jeweils aktuelle von DeepCloud zur Verfügung gestellte Version der DeepID App installiert sein.

8.4 Er verpflichtet sich, alle zumutbaren und zeitgemässen Möglichkeiten zu nutzen, sein Authentisierungsmittel gegen Angriffe und Schadsoftware ("Viren", "Würmer", "Trojaner" und dergleichen) zu schützen, insbesondere durch Verwendung stets aktueller Software aus offizieller Quelle.

8.5 Das Authentisierungsmittel muss entsprechend den Vertragsbedingungen des Herstellers und sachgemäss genutzt werden, namentlich sind alle Handlungen zu unterlassen, die durch die Veränderung oder das Ersetzen der vom Gerätehersteller installierten Gerätesoftware Risiken begünstigen oder verursachen (z.B. durch einen «Jailbreak/Rooting» oder andere Software, welche vom Hersteller vorgegebene Nutzungsbedingungen verletzt). Der Nutzer verpflichtet sich, Software (insbesondere andere Apps) ausschliesslich aus vertrauenswürdigen Quellen auf seinem Authentisierungsmittel zu installieren.

8.6 Das Betriebssystem auf dem Authentisierungsmittel muss dem offiziell durch den Hersteller zur Verfügung gestellten Stand entsprechen und mit der DeepID App kompatibel sein, ansonsten wird die DeepID App nicht unterstützt. DeepID setzt eine aktive Verbindung zum Netzwerk eines Mobilfunk-Diensteanbieters voraus. Die unterstützen Versionen des jeweiligen Betriebssystems werden in den entsprechenden App-Stores angezeigt.

8.7 Der Nutzer ist verpflichtet, zu jedem Zeitpunkt im Rahmen des Identifikationsprozesses und bei Nutzung seiner bestätigten Identität vollständige, richtige und aktuelle Angaben zu machen und Änderungen umgehend nachzupflegen. DeepCloud behält sich das Recht vor, Nachweise für die Richtigkeit der Angaben des Nutzers zu verlangen und selbst Nachprüfungen vorzunehmen. Die Unterrichtungspflicht betrifft insbesondere folgende Umstände: Name, Nationalität, Geschlecht, Wohnsitz, Kontaktangaben wie E-Mail-Adresse, Telefon, Änderung des Ausweispapiers und des Authentisierungsmittels bei Verlust, Diebstahl, Wechsel sowie jeden anderen faktischen oder Rechtsumstand, der Einfluss auf die Identifikation des Nutzers und das Nutzungsverhältnis mit DeepCloud haben könnte.

8.8 Die Nutzungsmöglichkeiten der mittels DeepID App bestätigten Identität und die jeweiligen Voraussetzungen für deren Einsatz ergeben sich aus dem jeweiligen Vertrag, den der Nutzer mit DeepCloud oder einem Drittanbieter schliesst.

8.9 DeepID kann nur für einen Dienst verwendet werden, welcher seine mittels DeepID bestätigte Identität auch akzeptiert. Ausserdem hat der Nutzer die jeweiligen Vertragsbestimmungen dieser Dienste zu akzeptieren, die gesondert gelten. Allfällige zusätzliche Voraussetzungen sind seitens des Nutzers strikt einzuhalten.

8.10 Der Nutzer ist verpflichtet, bestimmte Dienste nur dann in Anspruch zu nehmen, wenn er die angeforderten Voraussetzungen erfüllt. So ist es ihm nur gestattet, eine Beauftragung zur Erstellung einer FES oder QES einer Anbieterin vorzunehmen, wenn er die dafür erforderlichen Ausweispapiere für die Identifikation verwendet hat und über den geforderten Wohnsitz verfügt. Sollte er entsprechende Bestätigungen abgeben, obwohl diese nicht zutreffen, schliessen DeepCloud und die jeweiligen Drittanbieter jegliche Gewährleistung und Haftung für die erbrachten Dienste wie die Erteilung einer QES oder FES aus und behalten sich entsprechende rechtliche Schritte gegen den Nutzer vor. Zudem wird der Nutzer in einem solchen Fall sowohl DeepCloud als auch den entsprechenden Drittanbieter von allen Ansprüchen Dritter freistellen, die sich aufgrund der fehlerhaften Angaben des Nutzers ergeben.

8.11 Für die Nutzung von DeepID stellen einerseits die Kenntnis des DeepID PINs, des Wiederherstellungscodes bzw. der Zugriffschutz des Gerätes und andererseits der Besitz des Authentisierungsmittels persönliche Sicherheitselemente dar, deren Schutz in der Verantwortung des Nutzers liegt.

8.12 Um den Schutz gegen missbräuchliche Verwendung von DeepID und der bestätigten Identität sicherzustellen, dürfen bei der Auswahl des DeepID- bzw. Geräte-PINs keine trivialen oder gängigen Kombinationen (z.B. 123456) oder anderweitig mit geringem Aufwand ermittelbare Zahlenkombinationen - wie Telefonnummer, Geburtsdatum, Autokennzeichen - gewählt werden.

8.13 Der Nutzer ist verantwortlich für den Schutz seiner Zugriffsdaten, insbesondere für die Wahl eines sicheren PINs, die Sicherung seines Wiederherstellungscodes, wie auch für den Schutz vor Zugriffen Dritter auf das Authentisierungsmittel und die darauf installierte DeepID App. Sicherheitsrelevante Informationen müssen geheim gehalten werden und dürfen keinen anderen Personen bekannt gemacht werden (auch nicht dem jeweiligen Drittanbieter). Allfällige Aufzeichnungen von Zugriffsdaten sind sicher und getrennt vom Authentisierungsmittel aufzubewahren oder zu verschlüsseln sowie vor Zugriffen Dritter zu schützen.

8.14 Wenn der Nutzer weiss oder den begründeten Verdacht hat, dass ein Dritter Kenntnis seiner Zugriffsdaten hat, muss er diese unverzüglich in den Geräteeinstellungen ändern und wenn nötig, DeepCloud umgehend über den Vorfall informieren.

8.15 Wenn das Authentisierungsmittel gestohlen wurde bzw. abhandengekommen ist oder wenn der Nutzer weiss oder vermutet, dass eine andere Person Kenntnis der Zugriffsdaten erlangt hat (Kompromittierung), ist er zu folgendem verpflichtet: er muss die DeepID durch Mitteilung an den Support sperren lassen, er verzichtet unverzüglich auf die Nutzung seiner bestätigten Identität und der Dienste, die seine Autorisierung und Authentifizierung erfordern, wie das Erstellen von FES und QES, er lässt unverzüglich das Zertifikat für die Erstellung von Signaturen für ungültig erklären, er ändert gegebenenfalls seine Zugriffsdaten (z.B. bei DeepCloud in der DeepID App, im DeepCloud-Konto oder beim jeweiligen Drittanbieter).

8.16 Sobald es Änderungen an einem für die Authentisierung verwendeten Gerät (z.B. des Geräts an sich, E-Mail-Adresse) oder bei den massgeblichen Daten für seine Identifikation (wie Name, Nationalität, andere Attribute) gibt, informiert der Nutzer direkt DeepCloud, entweder durch die Nutzung «Ich habe bereits eine DeepID», «Dokument erneuern» oder durch Anpassungen der Daten in seinem Profil. Sollte dies nicht gelingen, wendet er sich unverzüglich an den DeepCloud Support. DeepCloud wird dann die relevanten Schritte unternehmen und die Anbieterinnen von Zertifizierungs- bzw. Vertrauensdiensten informieren, damit seine bestätigte Identität sowie das Zertifikat für ungültig erklärt werden können. Der Nutzer wird die erforderlichen Schritte bei seinen anderen betroffenen Diensteanbietern vornehmen.

8.17 Der Nutzer verpflichtet sich, seine Angaben zu seiner Identität nach ihrer Bestätigung fortlaufend zu prüfen und allfällige Unstimmigkeiten sowie den Verdacht einer missbräuchlichen Nutzung der DeepID Identität DeepCloud unverzüglich zu melden.

8.18 Dem Nutzer ist es strikt untersagt, DeepID für widerrechtliche Zwecke zu nutzen, so darf er für den Identifikationsprozess keine gefälschten oder fremden Ausweispapiere verwenden. DeepCloud behält sich in solchen Fällen die Untersagung der Nutzung von DeepID sowie die Vornahme rechtlicher Schritte gegen den Nutzer vor.

8.19 Verstösst der Nutzer gegen seine ihm obliegenden Pflichten, übernimmt er alle Risiken, die durch die Pflichtverletzungen begünstigt oder verursacht werden.

8.20 Wenn der Nutzer nicht mit den bei DeepID stattfindenden Datenverarbeitungen einverstanden ist, darf er DeepID nicht nutzen.

8.21 Ob Drittanbieter oder DeepCloud bei ihrer Diensterbringung unter Nutzung von DeepID eine Gebühr verlangen, richtet sich nach dem Vertrag zwischen dem Nutzer und DeepCloud oder dem jeweiligen Diensteanbieter. Zusätzlich können Kosten für den Datentransfer seitens des Mobilfunk-Diensteanbieters des Nutzers anfallen, wofür der Nutzer verantwortlich ist.

9. Support

9.1 Support wird nur während der üblichen Supportzeiten von DeepCloud (wie in Form von Foren oder FAQ, per E-Mail) erbracht. Der DeepCloud Support ist erreichbar unter support@deepid.swiss

9.2 Sollte es Auffälligkeiten oder Sicherheitsvorfälle bei den jeweiligen Identifikations-, Autorisierungs- oder Authentifizierungsprozessen geben, hat sich der Nutzer unverzüglich an DeepCloud zu wenden.

9.3 DeepCloud bietet keine Gewähr, dass Identifikationen, Autorisierungen oder Authentifizierungen (wie für die Beauftragung einer elektronischen Signatur) jederzeit rechtzeitig erfolgen können.

9.4 Bei Fragen zu den technischen Voraussetzungen, den Funktionalitäten von DeepID oder bei Störungen der Nutzung kann der Support ebenfalls kontaktiert werden.

9.5 DeepCloud behält sich vor, ihre Dienstleistungen im Rahmen des Supports nach ihren jeweils aktuellen Stundensätzen abzurechnen. Details zum Support und den konkreten Supportzeiten finden sich auf den Webseiten von DeepCloud.

10. Nutzungsdauer der bestätigten Identität

10.1 Unter Berücksichtigung der Voraussetzungen nach diesen AB sowie den AB der DeepCloud für ein DeepCloud-Konto kann der Nutzer seine bestätigte Identität mit dem während der Identifikation hinterlegten Authentisierungsmittel während einer Dauer von maximal fünf Jahren für Zertifizierungs- bzw. Vertrauensdienste nutzen, wobei sich diese Dauer entsprechend verkürzt, wenn die Gültigkeitsdauer des vom Nutzer vorgelegten Ausweispapiers früher abläuft, das Zertifikat der Anbieterinnen der Zertifizierungs- bzw. Vertrauensdienste abläuft oder ein anderer Umstand eintritt, der eine Re-Identifikation erforderlich macht.

10.2 Für andere Authentifizierungen als für Zertifizierungs- bzw. Vertrauensdienste kann es ebenfalls zeitliche Begrenzungen, auch aufgrund der Nutzungsbedingungen von Drittanbietern, geben. In allen anderen Fällen liegt es im Ermessen von DeepCloud, die Nutzungszeit für eine bestätigte Identifikation festzulegen, einschliesslich einer allfällig erforderlichen Re-Identifikation des Nutzers.

11. Datenschutz und Vertraulichkeit

11.1 DeepCloud wird die Bestimmungen des anwendbaren Datenschutzrechts im Rahmen ihrer Datenbearbeitungen einhalten. Sie gestaltet in ihrem Verantwortungsbereich ihre betriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie trifft technische und organisatorische Massnahmen zur angemessenen Sicherung der Daten des Nutzers vor Missbrauch und Verlust, die den Anforderungen des Datenschutzrechts entsprechen.

11.2 DeepCloud wird alle nicht allgemein bekannten Informationen, die sie über den Nutzer und seine Geschäftsbeziehungen erfährt, vertraulich behandeln. Sie wird diese Informationen Dritten nur sofern und so weit zugänglich machen, wie es aus dem Nutzungsverhältnis oder gesetzlich erlaubt ist, der Nutzer dies ausdrücklich erlaubt hat oder dies aufgrund behördlicher oder richterlicher Anordnung sowie gesetzlicher Pflicht erforderlich wird. Sie stellt ebenfalls die Einhaltung der Vertraulichkeitsverpflichtung aller im Zusammenhang mit diesem Nutzungsverhältnis involvierten Mitarbeitenden und beigezogenen Dritten sicher.

11.3 DeepCloud erhebt, speichert und bearbeitet neben den gemäss den geltenden Vorschriften erhobenen Daten, die für die Erbringung eines Zertifizierungs- bzw. Vertrauensdienstes benötigt werden, alle Daten und Informationen, die sie zur Erbringung ihrer Dienste für den Nutzer benötigt. Der Umgang mit diesen Daten richtet sich neben den jeweils anwendbaren Gesetzen auch nach den Zertifikatsrichtlinien für die Zertifizierungs- bzw. Vertrauensdienste.

11.4 DeepCloud zieht für ihre Dienste im Zusammenhang mit der Identifikation des Nutzers Dritte bei. Es handelt sich dabei um Auftragsdatenbearbeitungen im Auftrag von DeepCloud. DeepCloud hat die hierfür erforderlichen datenschutzrechtlichen Vereinbarungen mit diesen Dritten geschlossen.

11.5 Der Umgang mit personenbezogenen Daten von DeepCloud ist in ihrer Datenschutzerklärung auf ihrer Webseite beschrieben. Es gilt die jeweils aktuell veröffentlichte Fassung.

11.6 Gestützt auf die Daten, die im Identifikationsprozess vom Nutzer angegeben und von DeepCloud erhoben werden, stellt die jeweilige Anbieterin eines Zertifizierungs- bzw. Vertrauensdienstes auf Anfrage und mit Willensbekundung des Nutzers ein qualifiziertes oder fortgeschrittenes Zertifikat aus, welches erforderliche Angaben über den Nutzer enthält.

11.7 DeepCloud bewahrt die oben beschriebenen Daten sowie die Mittel anhand derer die Identität geprüft worden ist nach vertraglichen und gesetzlichen Aufbewahrungspflichten auf, auch damit der Nutzer einen Zertifizierungs- bzw. Vertrauensdienst nutzen kann. Die Aufbewahrungsfrist beträgt bei QES nach ZertES 11 Jahre und nach eIDAS VO 30 Jahre, im Falle von FES - sowohl nach ZertES als auch nach eIDAS VO - 7 Jahre. Aufgrund der maximalen Gültigkeitsdauer einer Identifikation von 5 Jahren führt dies unter Berücksichtigung einer zusätzlichen Sicherheitsfrist von einem Jahr zu Aufbewahrungsfristen für QES von bis zu 17 Jahren nach ZertES und bis zu 36 Jahren nach eIDAS VO sowie für FES bis zu 13 Jahren - sowohl nach ZertES als auch nach eIDAS VO.

11.8 Mit diesen Aufbewahrungsfristen wird sichergestellt, dass die Nachvollziehbarkeit der Korrektheit eines elektronisch signierten Dokuments in den Jahren nach deren Erstellung aufrechterhalten werden kann. Es werden hierbei alle einschlägigen Informationen über die ausgegebenen und empfangenen Daten aufgezeichnet und so aufbewahrt, dass sie verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können und die Kontinuität des Zertifizierungs- bzw. Vertrauensdienstes sicherzustellen.

11.9 DeepCloud löscht die erforderlichen Daten nach Ablauf von frühestens 17 Jahren nach ZertES und nach Ablauf von frühestens 36 Jahren nach eIDAS VO ab Durchführung des Identifikationsprozesses. Im Falle einer Identifikation nur nach Anforderung von FES löscht DeepCloud diese Daten nach Ablauf von frühestens 13 Jahren ab Durchführung des Identifikationsprozesses - sowohl nach ZertES als auch nach eIDAS VO. Eine Löschung der Daten kann erst nach Ablauf bestehender Aufbewahrungspflichten erfolgen.

11.10 Zum Zwecke der Information des Nutzers, dass die Nutzungsdauer der bestätigten Identität und eine mögliche Signaturerlaubnis abläuft, speichert DeepCloud den Zeitpunkt, wann dies der Fall sein wird, und informiert den Nutzer schriftlich oder auf andere Weise (z.B. innerhalb seiner DeepID App, eines bestehenden DeepCloud-Kontos oder mittels E-Mail) über diesen Umstand, damit er rechtzeitig eine Re-Identifikation vornehmen kann. Der Nutzer ist hiermit ausdrücklich einverstanden.

11.11 Sofern Daten benötigt werden könnten, um Drittanbieter oder DeepCloud gegen etwaige Schadenersatzansprüche zu verteidigen, werden diese für die Dauer allfälliger Verjährungsfristen aufbewahrt.

11.12 Der Nutzer hat die Möglichkeit für diverse Zwecke eine Weitergabe von Daten, Dokumenten und Informationen an Dritte im Rahmen einer Authentifizierung mittels DeepID freizugeben, mit oder ohne Verwendung von Drittanbieterdiensten, wie die Übermittlung von Daten an einen potenziellen Arbeitgeber, eine Versicherung oder Bank. Er kann ebenfalls seine bestätigte Identität verwenden, um sich als Vertretungsberechtigter einer Organisation zu authentifizieren. Wie Drittanbieter die Daten des Nutzers verarbeiten und welche Einflussmöglichkeiten er hierbei hat, sind den Datenschutzbestimmungen dieser Drittanbieter zu entnehmen. DeepCloud ist für diese Datenverarbeitungen nicht verantwortlich.

12. Beizug Dritter

12.1 DeepCloud kann jederzeit Dritte zur ordnungsgemässen Erfüllung ihrer Pflichten beiziehen, was der Nutzer hiermit genehmigt. Diese Dritten werden sorgfältig ausgewählt und durch DeepCloud beauftragt. Sie sind an Weisungen gebunden und werden regelmässig kontrolliert. Insbesondere werden Hosting sowie Service Provider mit Serverlösungen in der Schweiz beigezogen, deren Unternehmenssitz sich in der Schweiz bzw. der EU befindet.

13. Gewährleistung

13.1 DeepCloud bietet dem Nutzer eine getreue und sorgfältige Ausführung ihrer Dienste gemäss diesen AB.

13.2 DeepCloud gewährt weder allgemein noch zu einem bestimmten Zeitpunkt einen ununterbrochenen oder störungsfreien Betrieb von DeepID (inkl. der DeepID App) und die Nutzung ihrer Funktionalitäten. Die Gewährleistung bei DeepID (inkl. der eingesetzten App, Software, Hosting, etc.) wird - soweit gesetzlich zulässig - ausgeschlossen. DeepID wird «wie es ist» zur Verfügung gestellt.

13.3 DeepCloud ist bemüht, DeepID ohne Unterbrechungen zur Verfügung zu stellen. Allerdings kann die unterbrechungsfreie Verfügbarkeit nicht garantiert werden. DeepCloud kann jederzeit die Verfügbarkeit von DeepID vorübergehend beschränken oder unterbrechen, vor allem wenn dies im Hinblick auf Kapazitätsgrenzen, die Sicherheit oder Integrität der Server oder zur Durchführung technischer Wartungs- oder Instandsetzungsmassnahmen erforderlich ist oder dies der ordnungsgemässen oder verbesserten Erbringung der Leistungen dient. Sie bemüht sich hierbei um Berücksichtigung der Interessen des Nutzers und wird, soweit möglich, den Nutzer über Unterbrechungen mit angemessener Vorankündigung informieren.

13.4 Kostenlos erbrachte Dienste werden ohne Erfüllungs- oder Gewährleistungsansprüche erbracht. DeepCloud kann kostenlos zur Verfügung gestellte Dienste jederzeit und ohne Vorankündigung einstellen, ändern oder nur noch gegen Bezahlung anbieten. Daraus ergeben sich keinerlei Ansprüche oder Rechte des Nutzers.

13.5 Es bestehen keinerlei Garantien, dass DeepID den individuellen Bedürfnissen des Nutzers entspricht, unabhängig davon, ob diese DeepCloud mitgeteilt wurden. Angaben auf der DeepCloud Webseite oder sonstige werbliche Aussagen von DeepCloud stellen keine Beschaffenheitsangaben oder Garantien dar.

13.6 DeepCloud - in der Rolle einer Registrierungsstelle - hat mit dem Identifikationsprozess als Teil eines Zertifizierungs- bzw. Vertrauensdienstes die Anforderungen, die das Gesetz und die technischen Standards an solche Dienste stellen, zu erfüllen. DeepCloud setzt hierfür angemessene und dem aktuellen Stand der Technik entsprechende Sicherheitsmassnahmen ein. DeepCloud ist für die Beurteilung und Spezifizierung der Anforderungen aus anwendbaren Gesetzen und Regulatorien verantwortlich.

13.7 Der Nutzer nimmt zur Kenntnis, dass trotz aller Anstrengungen von DeepCloud, des Einsatzes moderner Technik und Sicherheitsstandards sowie der Kontrolle durch eine unabhängige Stelle betreffend die Einhaltung der technischen Standards und gesetzlichen Vorschriften eine absolute Sicherheit und Fehlerlosigkeit des Identifikationsprozesses und der Zertifizierungs- bzw. Vertrauensdienste nicht gewährleistet werden kann.

13.8 DeepCloud bietet keine Gewähr, dass eine Identifikation, Verifikation, Autorisierung oder Authentifizierung jederzeit durchgeführt und abgeschlossen werden kann und schliesst jegliche Haftung für mögliche Schäden aufgrund einer verspäteten, unterlassenen oder nicht erfolgreich abgeschlossenen Identifikation, Verifikation, Autorisierung oder Authentifizierung - soweit gesetzlich zulässig - aus.

14. Haftung und höhere Gewalt

14.1 DeepCloud haftet nur bei Vorsatz, grober Fahrlässigkeit sowie für Personenschäden. Im Übrigen ist jede weitere Haftung ausdrücklich ausgeschlossen, insbesondere diejenige für leichte Fahrlässigkeit, Folgeschäden, Vermögensschäden, immaterielle und indirekte Schäden (wie der ganze oder teilweise Verlust von Dokumenten oder Daten, Mehraufwendungen, entgangener Gewinn, Schäden durch Störungen der Verfügbarkeit, Ansprüche Dritter usw.) sowie für Hilfspersonen (inkl. beigezogene Dritte). Dies gilt ebenfalls für eine allfällige verschuldensunabhängige Haftung.

14.2 DeepCloud übernimmt keine Haftung für die ständige Verfügbarkeit der DeepID App, ihres Supports, angebotener Prozesse und Einsatzmöglichkeiten sowie der einzelnen Funktionalitäten der DeepID App.

14.3 DeepCloud haftet dem Nutzer gegenüber nicht für das ordentliche Funktionieren von Systemen Dritter, insbesondere nicht für die vom Nutzer verwendete Hard- und Software oder für einen von ihm genutzten Drittanbieterdienst unter Verwendung seiner bestätigten Identität zur Authentifizierung.

14.4 Es besteht keine Haftung, wenn die Erbringung ihrer Leistung auf Grund höherer Gewalt zeitweise unterbrochen, ganz oder teilweise beschränkt oder unmöglich ist. Als höhere Gewalt gelten insbesondere Naturereignisse von besonderer Intensität (Lawinen, Überschwemmungen, Erdrutsche usw.), kriegerische Ereignisse, Aufruhr, unvorhersehbare behördliche Restriktionen sowie Pandemien oder Epidemien. Kann DeepCloud ihren Verpflichtungen nicht nachkommen, wird deren Erfüllung oder der Termin für die Erfüllung dem eingetretenen Ereignis entsprechend hinausgeschoben. DeepCloud haftet nicht für allfällige Schäden, die dem Nutzer durch das Hinausschieben der Erfüllung entstehen.

14.5 Allfällige Ansprüche muss der Besitzer innert sechs Monaten nach Leistungserbringung geltend machen.

14.6 Diese Haftungsausschlüsse und Haftungsbeschränkungen gelten für vertragliche als auch für ausservertragliche Ansprüche des Besitzers.

14.7 DeepCloud haftet nicht für Schäden aus vertrags- oder rechtswidriger Nutzung von DeepID durch den Nutzer.

14.8 Ausgenommen von diesen Haftungsbeschränkungen und Haftungsausschlüssen sind zwingend bestehende Haftungsregelungen aufgrund von Produkthaftgesetzen, Verbraucherschutzgesetzen, ZertES oder eIDAS VO sowie deren Ausführungsgesetzen. Es gelten in solchen Fällen, die in diesen Bestimmungen allfällig vorgesehenen Haftungsbegrenzungen und Haftungsausschlüsse ebenfalls für DeepCloud.

14.9 DeepCloud hat ihre Haftung im Hinblick auf die Nutzung von DeepSign in ihren Allgemeinen Bestimmungen für die Nutzung des DeepCloud-Kontos und der DeepServices gegenüber dem Nutzer geregelt.

14.10 Der Nutzer haftet insbesondere und stellt DeepCloud von jeglichen (Schadensersatz-) Ansprüchen im Zusammenhang mit der Nutzung von DeepID frei, die darauf beruhen, dass er gegen anwendbare Gesetze und Vorschriften, die guten Sitten, diese AB oder Vertragsbestimmungen von DeepCloud oder Drittanbietern wie Zertifizierungs- bzw. Vertrauensdiensteanbieterinnen, verstösst.

15. Änderungen dieser AB

15.1 DeepCloud behält sich das Recht vor, die DeepID App sowie diese AB jederzeit zu ändern und zu ergänzen. Insbesondere bei Änderungen des ZertES, der eIDAS VO und ihren jeweiligen Ausführungsgesetzgebungen sowie bei Anordnungen der zuständigen Anerkennungs-, Bestätigungs- und Aufsichtsstelle oder einer unabhängigen Stelle zur Prüfung der Signaturen können die Zertifizierungs- bzw. Vertrauensdiensteanbieterinnen gezwungen sein, bestehende Zertifikatsrichtlinien und folglich DeepCloud als Registrierungsstelle diese AB anzupassen. Der Nutzer wird vor Geltungsbeginn der Änderungen von DeepCloud über allfällige Änderungen informiert oder es werden ihm bei Nutzung eines Dienstes, die jeweils aktuellen Bestimmungen angezeigt. Diese Information kann für den Nutzer in geeigneter Weise erfolgen.

15.2 Änderungen gelten als akzeptiert, wenn der Nutzer das Vertragsverhältnis nicht bis zum Inkrafttreten der neuen AB kündigt, auf jeden Fall aber bei Nutzung von DeepID nach Inkrafttreten der neuen Bestimmungen, trotz Möglichkeit der Kenntnisnahme der Änderungen.

15.3 Der Nutzer kann die Annahme der neuen Bedingungen auch ablehnen, indem er auf die Nutzung von DeepID (wie der bestätigten Identität, Autorisierungen sowie Authentifizierungen durch DeepID) gemäss diesen AB ab dem Geltungsbeginn der geänderten Bedingungen verzichtet.

15.4 Sollten sich einzelne Bestimmungen dieser AB als unwirksam oder nichtig erweisen, so hat dies nicht die Unwirksamkeit oder Nichtigkeit der übrigen Bestimmungen zur Folge, sondern diese werden durch solche ersetzt, die ihrem wirtschaftlichen Zweck am nächsten kommen. Das Gleiche gilt bei einer Lücke in den Nutzungsbestimmungen.

16. Inkrafttreten, Dauer und Beendigung

16.1 Das Nutzungsverhältnis mit dem Nutzer über DeepID kommt mit Akzeptieren dieser AB innerhalb der DeepID App zustande und besteht auf unbestimmte Zeit.

16.2 DeepCloud ist berechtigt, das Nutzungsverhältnis jederzeit ohne Angabe von Gründen zu beenden. Zum Zeitpunkt der Beendigung wird DeepCloud den Zugang zu DeepID und der bestätigten DeepID Identität sperren, ihre Nutzung beenden und die technische Kommunikation zu den DeepServices oder zu Diensten von Drittanbietern einstellen. Dies bedeutet insbesondere, dass alle noch hängigen Dienste sowie allfällig dazugehörende Statusmeldungen und Informationen nicht mehr transportiert bzw. nicht mehr ausgeführt werden oder zur Verfügung stehen.

16.3 Der Nutzer kann jederzeit auf die Nutzung von DeepID verzichten und die DeepID App von seinem Authentisierungsmittel löschen. Der Nutzer ist für die Planung der Beendigung der Nutzung von DeepID und seiner DeepID Identität selbst verantwortlich. Hinsichtlich der Sperrung seiner DeepID Identität oder der Löschung von Daten wendet sich der Nutzer an DeepCloud.

16.4 Bei Beendigung des Nutzungsverhältnisses stehen dem Nutzer seine bestätigte Identität sowie die Nutzung von DeepID nicht mehr zur Verfügung.

17. Anwendbares Recht und Gerichtsstand

17.1 Alle Rechtsbeziehungen im Zusammenhang mit diesen AB unterstehen dem schweizerischen Recht unter Ausschluss des internationalen Privatrechts und des Wiener Kaufrechts, unabhängig davon, ob ein Nutzer DeepID in seiner Eigenschaft als Verbraucher oder für ein Unternehmen nutzt.

17.2 Ist der Nutzer ein Verbraucher mit gewöhnlichem Aufenthalt in der EU/EWR, gilt ansonsten ergänzend das zwingende Verbraucherschutzrecht des EU/EWR Staates an seinem gewöhnlichen Aufenthalt in der EU/EWR. Dies gilt ebenfalls, sofern es sich um ein Land handelt, für das die eIDAS VO anwendbar ist.

17.3 Unter Vorbehalt zwingender Gerichtsstände ist für alle Streitigkeiten aus oder in Zusammenhang mit diesen AB die Stadt St. Gallen der ausschliessliche Gerichtsstand.

18. Schlussbestimmungen

18.1 Der Nutzer kann keine Rechte aus diesem Nutzungsverhältnis auf Dritte übertragen. DeepCloud ist berechtigt, alle Rechte und Pflichten aus diesem Nutzungsverhältnis an Dritte zu übertragen. Der Nutzer stimmt hiermit einer allfälligen Abtretung oder Übertragung zu.

18.2 Im Falle von Streitigkeiten bemühen sich die Parteien um eine gütliche Beilegung der Streitigkeit.

18.3 Alle Personenbezeichnungen in diesen AB sind gender-neutral zu verstehen.

18.4 Diese AB liegen in unterschiedlichen Sprachen vor. Bei Abweichungen oder Widersprüchen ist die deutsche Fassung massgeblich.

19. Zwingendes EU/EWR-Verbraucherschutzrecht

19.1 Die Widerspruchsfrist betreffend Änderungen dieser AB für Nutzer, auf welche zwingendes EU/EWR-Verbraucherschutzrecht ergänzend anwendbar ist, beträgt 4 Wochen.

19.2 DeepCloud kann das Nutzungsverhältnis ordentlich jederzeit zum Monatsletzten beenden – dabei gilt eine 30-tägige Kündigungsfrist.

19.3 Wenn es sich bei dem Nutzer um einen Verbraucher in der EU/EWR handelt, ist DeepCloud weder bereit noch verpflichtet, an einem Verfahren der Streitbeilegung vor einer Verbraucherschlichtungsstelle teilzunehmen. Verbraucherinformation gemäss Verordnung (EU) Nr. 524/2013: Zum Zwecke der aussergerichtlichen Beilegung von Verbraucherstreitigkeiten hat die Europäische Kommission eine Plattform für Online-Streitbeilegung (OS-Plattform) eingerichtet. Die OS-Plattform ist unter https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=DE erreichbar.